

Manual de instalação

Certificado Digital A3 ou S3

CERTISIGN
A sua identidade na rede

Sumário

O que é?

O Certificado Digital é uma credencial que identifica uma pessoa física ou entidade, seja empresa, máquina, aplicação ou site.

O certificado é um documento eletrônico seguro, que permite ao usuário se comunicar e efetuar transações na internet de forma mais rápida e sigilosa.

Portanto **NÃO** entregue seu Certificado Digital ou senhas para outras pessoas.

Como sua assinatura de próprio punho, a assinatura digital tem validade jurídica. Isso significa que você concorda com os termos que assinou, garantindo autenticidade e integridade às informações neles contidas.

Aplicação

Por se tratar de um documento eletrônico, o Certificado Digital se tornou um recurso bastante utilizado em diversos segmentos como governo, saúde, contabilidade, finanças, entre outros. Com a finalidade de agilizar processos com segurança e sigilo eliminando o uso de papel no envio de informações os certificados são utilizados, principalmente na Receita Federal do Brasil para o envio de declarações de imposto de renda (DIRF, DIPJ), consulta de situação fiscal e fontes pagadoras e principalmente procurações eletrônica.

Também é utilizado em operações para assinatura dos livros Fiscais SPED, processos enviados em cartórios de notas, juntas comerciais, prefeituras, peticionamento eletrônico e diversas outras aplicações que já estão disponibilizadas no mercado.

Além disso, a Receita Federal do Brasil criou uma solução para que outras pessoas possam atuar em seu nome: o e-CAC. Nesta aplicação é possível criar uma procuração eletrônica que discrimina os poderes aos seus representantes legais. Para mais informações, acesse o site www.receita.fazenda.gov.br

Preparando sua máquina

Antes de emitir seu certificado digital, é preciso preparar sua máquina.
A configuração do equipamento evita possíveis erros no momento da emissão.

1° passo: Sistemas Homologados

Os certificados digitais da Certisign podem ser utilizados em qualquer sistema operacional que possua suporte à certificação digital, porém **DEVEM** ser emitidos exclusivamente nos sistemas operacionais e navegadores abaixo:

Windows © XP [1] (com SP2 ou superior) ou Windows © 2000 (com SP4 ou superior) e Internet Explorer © 6.0 ou 7.0 .

2° passo: Perfil de usuário

Verifique se seu perfil de usuário possui privilégios para acessar e instalar novos componentes, tais como hardwares criptográficos e o próprio certificado digital. Caso não tenha certeza, chame o administrador da rede ou um técnico de sua confiança antes de iniciar o processo de emissão do certificado.



Imagem 01

3° passo: Execute CD de Instalação

Execute o CD de instalação recebido no momento da validação presencial.
Selecione seu dispositivo e siga os passos indicados.
Após a instalação do dispositivo, prossiga com o 4º passo, localizado na página 9 deste manual.

Caso não possua o Cd de Instalação, acesse www.certisign.com.br/suporte/utilitarios-criptograficos, e instale os dispositivos criptográficos e prossiga com o 5º passo, localizado na página 9 deste manual.

---

1 - Não funciona na versão Windows© XP Starter Edition.

4° passo: Hierarquias de Certificação

Este procedimento é necessário também nos casos de renovação do certificado

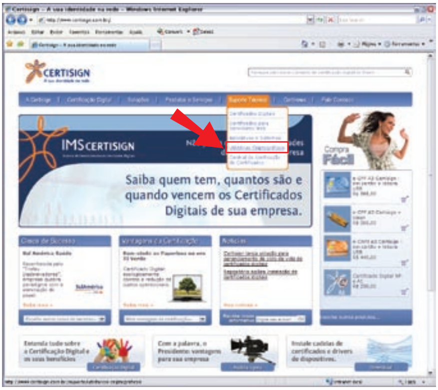


Imagem 02

1. Acesse o www.certisign.com.br e no menu, aponte para **"Suporte técnico"**, e, na sequência, clique em **"utilitários criptográficos"**;

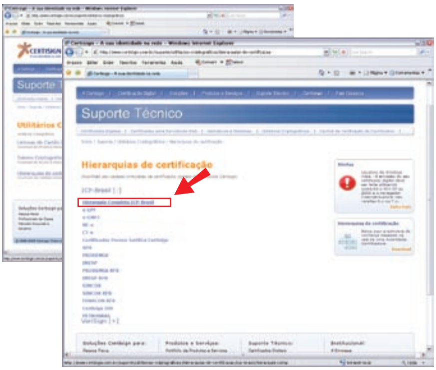


Imagem 03 e 04

2. Clique no link **"hierarquia de certificação"**;
3. Clique no link **"hierarquia completa ICP-Brasil"**;



Imagem 05

4. Na página seguinte clique no link **"instalador de certificados certisign"**;

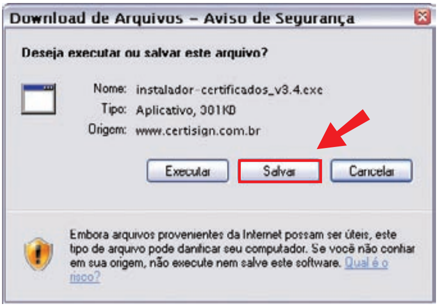


Imagem 06

5. Escolha a opção **"salvar"**;

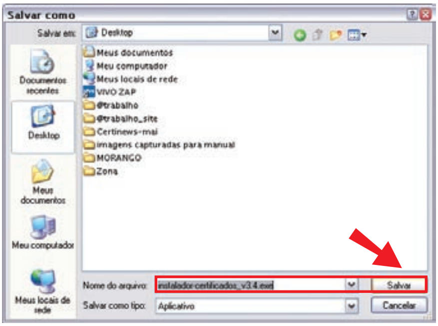


Imagem 07

6. Escolha o local onde deseja salvar o seu arquivo e clique em **"salvar"**;



Imagem 08

7. Aguarde até que o instalador carregue/salve o arquivo;



Imagem 09

8. Após o carregamento do instalador clique em **“Executar”**;

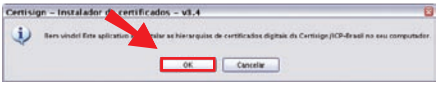


Imagem 10

9. Clique na opção **“ok”**;

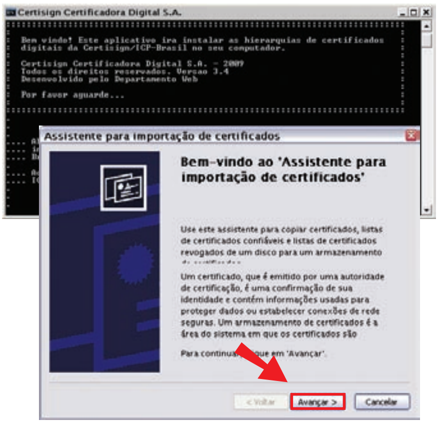


Imagem 11

10. Abrirá a janela do **“Assistente para importação de certificados”**, clique em **“Avançar”**;

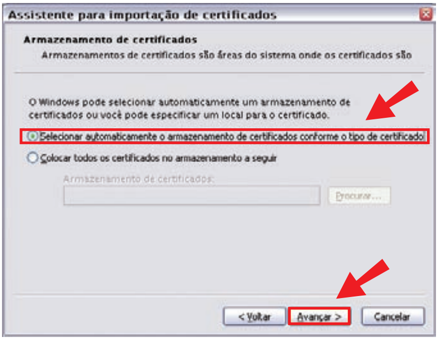


Imagem 12

11. Selecione a opção **"Selecionar automaticamente o armazenamento de certificados conforme o tipo de certificado"**, em seguida clique em **"Avançar"**;

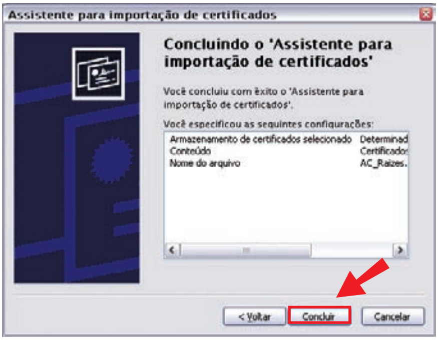


Imagem 13

12. Na tela ilustrada pela imagem 13, clique em **"concluir"**;

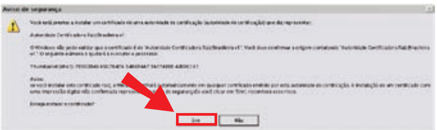


Imagem 14

13. Escolha **"Sim"**, para o aviso de segurança do Windows©;



Imagem 15

14. Pronto! A importação obteve êxito. Clique em **"ok"** ;

OBS: Este procedimento será realizado duas vezes para instalação das hierarquias ICP-Brasil.



Imagem 16

15. Tecle **"enter"** em todas as telas seguintes para concluir a instalação.

    Parabéns!
    Sua instalação foi concluída com êxito.

5° passo: Capicom

Capicom é um arquivo do windows necessário para assinar dados e verificar assinaturas digitais. Sua instalação deve ser feita diretamente pelo site da Microsoft®

1. Acesse http://www.microsoft.com.br

2. No campo de busca digite **CAPICOM SDK**, e tecle **"enter"**.

3. Selecione a opção: **"Detalhes do download: Platform SDK redistribuível: CAPICOM"**
   Será carregada a página ilustrada na imagem 17

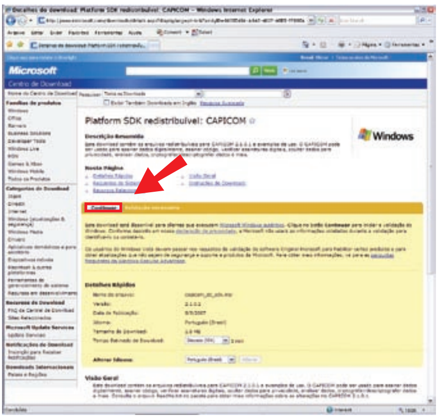


Imagem 17

4. Clique em **"Continuar"**, e siga os procedimentos descritos na tela;

5. Reinicie a máquina ao término da instalação.

6° passo: Internet explorer© 7.0

Se você utiliza este navegador realize os passos abaixo

ActiveX

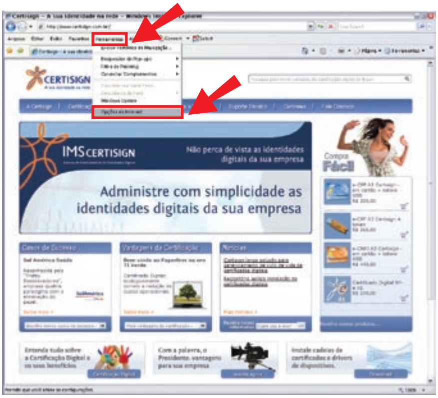


Imagem 18

1. Abra seu navegador de Internet (Internet Explorer© 7.0);

2. Clique no menu **“Ferramentas”** no topo da página; em seguida selecione a opção **“Opções da Internet”**;

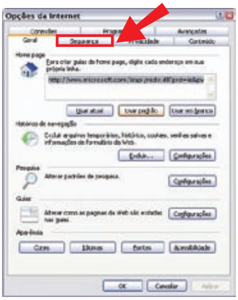


Imagem 19

3. Nessa nova janela, clique na aba **“Segurança”**;

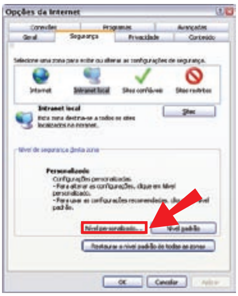


Imagem 20

4. Depois selecione o botão **“Nível Personalizado”**;

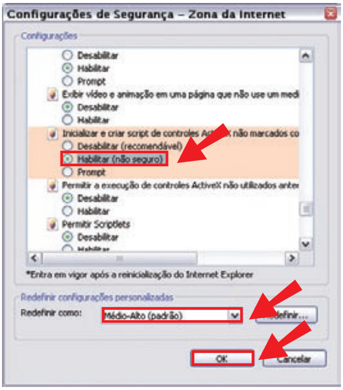


Imagem 21

5. Na janela **"Configurações de Segurança"**, redefina as configurações de segurança de **"médio-alto"** para **"médio"** e clique em **"redefinir"**;

6. Nessa mesma tela, localize o item **"Inicializar e criar Scripts de controles ActiveX não marcados como seguros para scripts"**, troque a opção deste item para **"Habilitar"** e clique em **"OK"**;

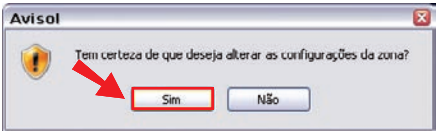


Imagem 22

7. Tecle **"sim"** para o Aviso do Windows©

Confiabilidade do site

1. Repita os passos de 1 a 3 da configuração de ActiveX para exibir a guia **"Segurança"** nas **"Opções de Internet"** em seu navegador de Internet (Internet Explorer© 7.0) (ver imagens 18 e 19);

2. Selecione a opção **"Sites Confiáveis"**;

3. Clique no botão **"Sites"**;



Imagem 23



Imagem 24

4. Nesta nova janela, digite o site: "https://gestaoar.certisign.com.br" e clique em **"Adicionar"**;

5. Feche as **"Opções de Internet"** e todos os navegadores abertos.

Emitindo o Certificado Digital

Agora que você já preparou o seu computador, vamos lhe auxiliar a emitir seu certificado digital

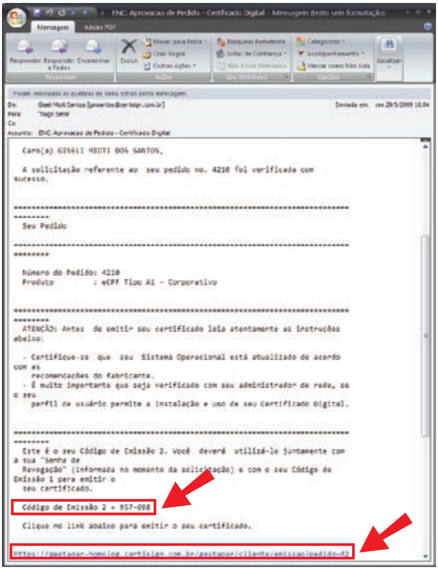


Imagem 25

1. Inicie o seu gerenciador de e-mails;

2. Abra o e-mail que foi enviado ao endereço cadastrado com o assunto **"Aprovação de pedido"**;

3. Abra o link de emissão, contido corpo da mensagem recebida, certificando-se que está utilizando o navegador Internet Explorer© 6.0 ou 7.0 ;

4. Este mesmo e-mail contém o código de emissão 2, que será usado juntamente com ao código de emissão 1 (entregue no momento da validação presencial);

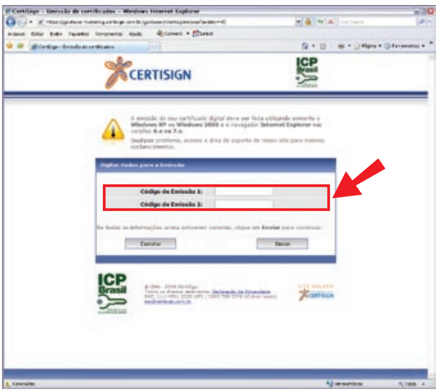


Imagem 26

5. Digite o **código de emissão 1** (6 dígitos);
   Obs.: não é necessário digitar o hífen (-).

6. Digite o **código de emissão 2** (6 dígitos), encontrado no e-mail **"Aprovação de pedido"**, conforme item 4;

   Obs.: Caso os códigos sejam digitados de maneira incorreta por 3 vezes, será necessário retornar ao ponto de atendimento para desbloquear o seu pedido.

   Esta medida visa garantir que pessoas não autorizadas sejam impedidas de obter o seu certificado.



Imagem 27

7. Após ter digitado os 2 códigos, clique em **“Enviar”**;



Imagem 28

8. Escolha o tipo de mídia que foi adquirida, selecione a mídia correta, e clique em **“Enviar”**;

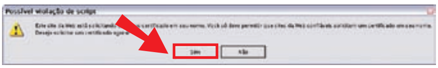


Imagem 29

9. Clique em **“sim”** para o aviso do Windows© sobre **“Possível violação de script”**;



Imagem 30

10. No caso do token Alladin o sistema solicitará a senha cadastrada no ato da validação presencial, digite a senha e clique em OK para avançar o processo de instalação.Clique **“OK”**, para concluir a instalação;

11. Atenção

Fique atento as senhas de sua mídia. Elas já podem ter sido alteradas no momento da validação presencial:

Midia	 Cartão	 iKey 2032 (Rainbow)	 e-Token Pro (Alladin)	 IKey 2032 (e-simples)
Senhas	1234	123456	123456	123456
Tentativas	3	10	15	10

Atenção

Caso seu token tenha sido formatado/ inicializado a senha retornará para a configuração de fábrica:

- e-TokenPro (Alladin) - 1234567890
- iKey 2032 (Rainbow) - PASSWORD

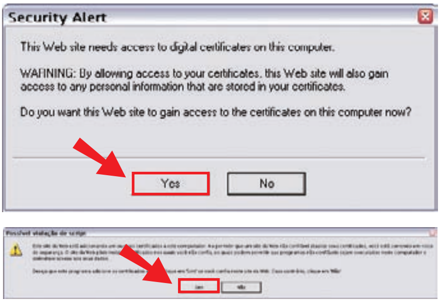


Imagem 31

12. Clique em **"Sim"** para os avisos de **"Alerta de segurança"** e **"Possível violação de script"**;



Imagem 32

13. Pronto! Seu certificado foi instalado com sucesso. Clique em **"ok"** para finalizar o processo

Testando seu Certificado

Teste se seu certificado está funcionando corretamente.



Imagem 34

1. Para isso acesse **www.certisign.com.br** e aponte para o menu suporte técnico, e clique em **"Central de Verificação de Certificados"**;



Imagem 35

2. Na pagina seguinte, clique em **"teste aqui seu certificado"**;

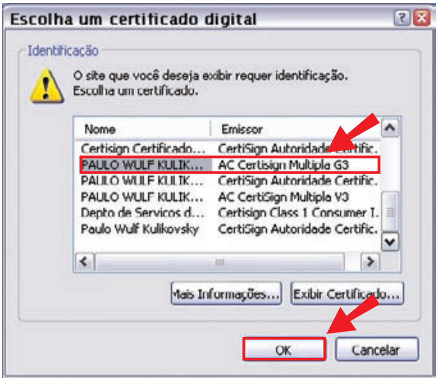


Imagem 36

3. Será exibida uma janela contendo os certificados que estão reconhecidos pela aplicação, como está ilustrado na imagem 36. Selecione seu certificado e clique em **"ok"**;



Imagem 37

4. Caso seja solicitado, insira a senha do seu certificado e clique em **"ok"**;

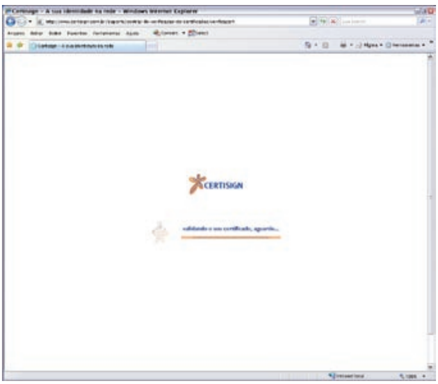


Imagem 38

5. Aguarde enquanto o sistema verifica seu certificado;

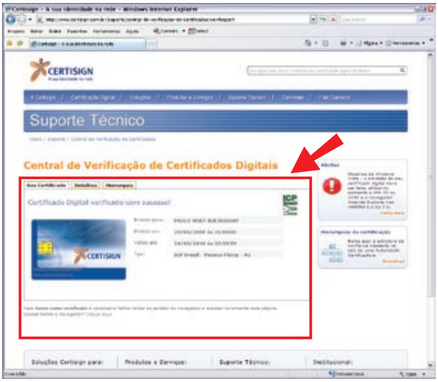


Imagem 39

6. Após a verificação do sistema, estarão disponíveis todas as informações referente ao seu certificado (emissão, validade...). Esta visualização demonstra que seu certificado está apto para utilização.

Em que momento será solicitada a senha de revogação?

A Senha de Revogação será solicitada na revogação ou renovação do certificado digital pela Internet.

É muito importante memorizá-la, pois sem ela não será possível revogar seu certificado digital on-line.

Em caso de perda da senha de revogação por qualquer motivo, a revogação requer o comparecimento em um dos nossos postos de atendimento.

Atenção

Nas seguintes situações, seu certificado será inutilizado e será necessário adquirir um novo, bem como agendar novo comparecimento a um ponto de atendimento para validá-lo:

- Perda do Cartão de Identidade ou Token;
- Formatação ou bloqueio das senhas PIN ou PUK de seu Cartão Inteligente;
- Perda ou bloqueio das senhas PIN ou *password* de seu Token;
- Inicialização ou remoção das chaves de seu Cartão ou Token;
- Formatação na máquina;
- Exclusão do perfil no qual o certificado foi instalado.

Caso ocorra problema durante a emissão do seu certificado acesse nosso atendimento online pelo site www.certisign.com.br/sac/chat ou entre em contato com nossa central de atendimento pelos telefones (11) 4501-2222 (São Paulo) e 0300 789 2378 (demais localidades).

Anotações